2026 Q1

LATVIAN CYBERSPACE SITUATION

PERIOD:

01.01.2026–31.03.2026

CERT.LV
Cyber Incident Response Institution

Institute of Mathematics and Computer Science University of Latvia

Ministry of Defence Republic of Latvia

Summary

In Q1 2026, the cybersecurity threat level in Latvia **remains high, requiring continued targeted measures to mitigate risks and strengthen resilience**. Since Russia's full-scale invasion of Ukraine in 2022, the number of registered cyber incidents in Latvian cyberspace has increased sixfold, while the number of identified compromised devices has increased eightfold.

A total of **846 cyber incidents** were processed manually – a decrease of 8% compared to the previous quarter, while still representing the second-highest figure recorded to date.

Identified compromised devices reached 757 286, the highest figure recorded to date. The majority of these are configuration weaknesses, highlighting vulnerabilities in system and network security, primarily caused by human factors and insufficient security standards. At the same time, this reflects not only an actual increase in threats but also **improved organisational cybersecurity capabilities in terms of visibility** at the **endpoint level**, enabled by the implementation of CERT.LV's Security Operations Centre (SOC) service and expanded compliance with national regulation. This enables the earlier detection, analysis, and mitigation of cyber risks, and systematically strengthens overall resilience.

Most observed cyber-attacks **did not result in significant or long-lasting consequences**. This is largely due to preventive cybersecurity measures and the overall resilience of Latvian cyberspace.

CERT.LV's DNS firewall **blocked access to malicious websites more than 2.5 million times** – this is 139% more than in the previous quarter and 416% more than in the same period last year. The decrease in the number of cyber incidents is also explained by the development of threat detection mechanisms. By continuing to develop automated detection capabilities, CERT.LV proactively identified and blocked 266 fraudulent campaigns, including preventing several near-incidents.

Latvian cyberspace experienced a full spectrum of cyber-attacks; quantitatively, the largest categories were fraud and malicious code. Meanwhile, distributed denial-of-service (DDoS) attacks against Latvian state and local government institutions and key service providers have become a constant operational risk, serving as a continuous stress test of capacity and resilience.

Dominant threats included phishing, information-stealing malware, fake software updates, and malicious browser extensions that bypass traditional protection mechanisms. The main risks were related to credential theft and unauthorised access.

Attacks are becoming increasingly automated and based on social engineering rather than purely technical vulnerabilities – further amplified by the growing capabilities of artificial intelligence, which accelerates fraud, intrusions, and automated attacks. The greatest challenge is not a single isolated threat, but the simultaneous occurrence of multiple risks.

A significant portion of cyber incidents were financially motivated. The activities of state-sponsored groups continue with varying intensity, including in relation to the geopolitical context. Russia continues to be the primary security threat, given Latvia's support for Ukraine in the war against Russian aggression.

Serious concern remains regarding threats from hostile states aiming to gain control over critical infrastructure systems and carry out disruptive actions that could affect or even halt essential services. To mitigate such risks and make Latvia a more difficult target, CERT.LV continues to develop operational technology activities, ensuring broader visibility, threat identification, security testing, and coordinated incident response.

The increasing intensity of attacks, more innovative attack methods, and geopolitically motivated incidents **clearly demonstrate the critical importance of cybersecurity**. CERT.LV services, including SOC monitoring, threat hunting, and regular security testing, significantly strengthen Latvia's cyber resilience. At the same time, by providing regular training and strengthening user knowledge in cybersecurity, CERT.LV experts educated **13 309** participants across **65** events during the reporting period.

As observed trends continue, priority should be given to strengthening endpoint security, resource capacity, user training, and supply chain control, while continuously improving response capabilities and operational continuity in line with regulatory requirements.

Key indicators

846 (+34%)

Manually processed
Cyber incidents
Q1 2026 vs Q1 2025

~754K (+167%)

Number of identified
compromised devices
Q1 2026 vs Q1 2025

556 (+39%)

Fraud –
dominant incident type
Q1 2026 vs Q1 2025

73 (+82%)

Malicious code –
fastest growth
Q1 2026 vs Q1 2025

~2,5M (416%)

Number of times CERT.LV DNS
firewall lists blocked access
to malicious websites
Q1 2026 vs Q1 2025

>84K (+9K)

DNS firewall mobile app downloads on
Android and iOS devices
Data as at the end of Q1 2026

92 (+37)

Total number of institutions
(NCL subjects) using
the CERT.LV SOC service
Data as at the end of Q1 2026

43 037 (+3%)

Number of endpoints with
visibility provided within
the CERT.LV SOC service
Data as at the end of Q1 2026

166 (+18)

Total number of registered security
researchers on the CVD platform
Data as at the end of Q1 2026

541 (+107)

Total number of vulnerability reports
registered on the CVD platform
Data as at the end of Q1 2026

65 (+32)

Cybersecurity awareness
activities/events conducted
by CERT.LV experts
Q1 2026 vs Q1 2025

13 309 (+3 104)

Audience reached through CERT.LV
expert activities/events
Q1 2026 vs Q1 2025

Contents

1. Cybersecurity threats: statistics and trends

Dynamics of cyber incidents and compromised devices

In Q1 2026, the cybersecurity threat level in Latvia remains high, requiring continued targeted efforts to mitigate risks and strengthen resilience. Since Russia's full-scale invasion of Ukraine in 2022, the number of cyber incidents registered in Latvian cyberspace[1] has increased sixfold, while the number of identified compromised devices has increased eightfold.

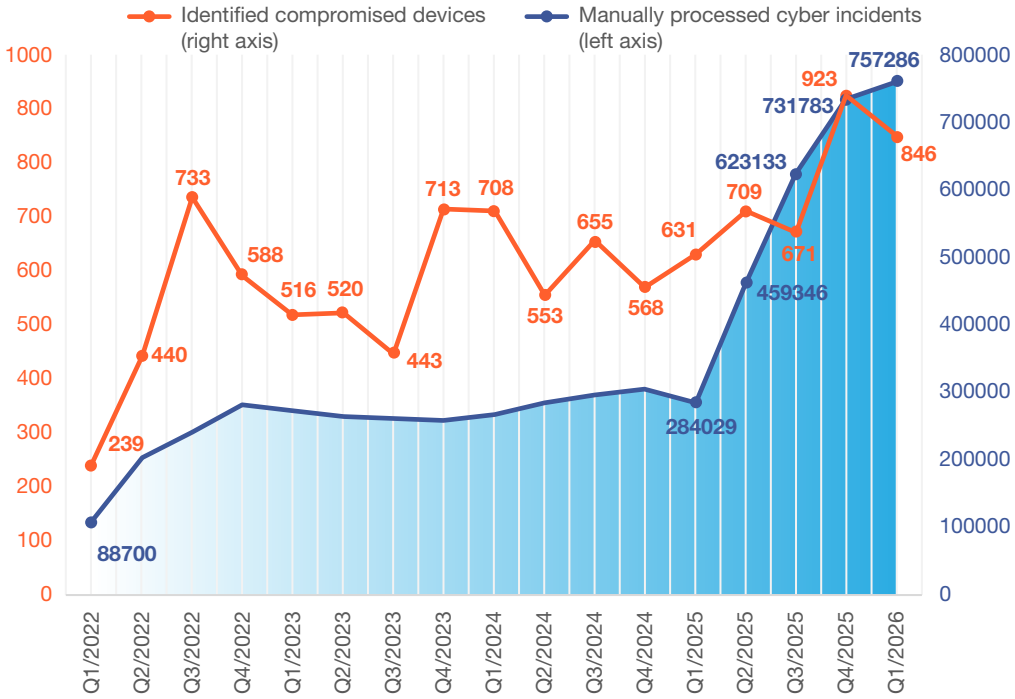

Figure 1. Dynamics of cyber incidents and identified compromised devices (number)

Manually processed cyber incidents

In Q1 2026, a total of **846 manually processed cyber incidents** were registered in Latvia – the second-highest figure recorded to date. Compared to Q1 2025, this represents an increase of 34%.

Compared to Q4 2025, the number of incidents decreased by 8%. A significant factor contributing to this decrease is the improved effectiveness of threat detection mechanisms. During the reporting period, **several fraudulent campaigns were proactively identified and mitigated**, including the prevention of multiple near-incidents . CERT.LV, continuing to develop automated detection mechanisms (analytical scripts) and DNS/domain reputation indicators, **proactively identified and blocked 266 active fraudulent campaigns** (predominantly campaigns abusing the identities of CSDD and banks), effectively **limiting their spread and preventing access to end users**.

Overall, the increase in cybersecurity threats in Latvian cyberspace correlates with the global escalation of cyber threats, increasing societal dependence on digital technologies, and the human factor. The continuous development of artificial intelligence (AI) tools also plays a significant role, facilitating and accelerating fraud, intrusions, and automated attacks.

1 **Cybersecurity incident** (hereinafter – cyber incident) – an event that threatens processed data or the availability, authenticity, integrity, or confidentiality of services offered by or accessible through network and information systems.
2 **Near cyber incident** – an event that could have threatened processed data or the availability, authenticity, integrity, or confidentiality of services offered by or accessible through network and information systems, but whose full execution was successfully prevented or did not materialise.

Identified compromised devices

The number of compromised devices identified by CERT.LV reached **757 286 – the highest figure recorded to date**, representing a 167% increase compared to Q1 2025 and a 3% increase compared to Q4. This trend suggests the growing use of automated scans and the exploitation of vulnerabilities. The majority consist of configuration weaknesses, highlighting vulnerabilities in system and network security, primarily caused by human factors and insufficient security standards.

The increase in the number of identified compromised devices is explained not only by an actual increase in threats but also by **significantly improved visibility at the endpoint level following the implementation of the CERT.LV SOC service**. At the same time, by expanding the client base in line with the entities defined in the National Cybersecurity Law (hereinafter – NCL) , **the number of monitored devices has increased**. These factors collectively contribute to timely threat identification and improve organisations' ability to ensure continuous, effective protection and resilience against cyber threats in 24/7 mode.

The beginning of 2026 shows that from January to March, the number of cyber incidents remains consistently high, indicating a sustained high baseline rather than isolated spikes. This means organisations must operate in a continuous resilience mode rather than reacting to isolated incidents only.

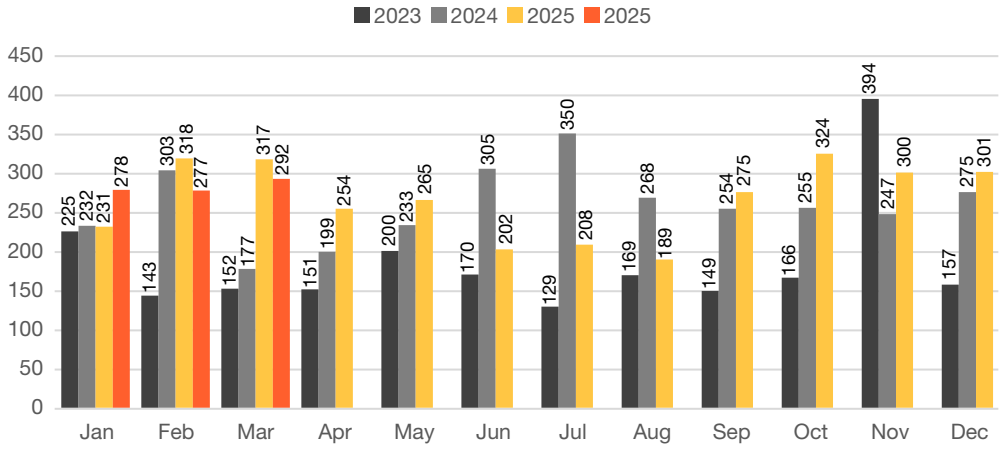

Figure 2. Cyber incident trends (monthly breakdown)

3 Essential service providers, important service providers, and owners and lawful operators of critical information and communication technology infrastructure (together hereinafter – NCL entities)

For "cyber weather" observers, CERT.LV offers a monthly report on the most significant and notable cyber incidents and threats in Latvian cyberspace across TOP 5 categories. The report is available on the CERT.LV website under the "News" section (JANUARY | FEBRUARY | MARCH)

2. Top reporting-period cyber threats and key events

TOP 5 cyber incident types by volume

Highest risk – fraud and malicious code. Showing rapid growth:

- Fraud increased by 39% (dominant incident type);
- Malicious code increased by 82% (fastest growth).

The number of compromised devices remained stable, while availability disruptions increased by 43%, indicating rising operational risks.

The decrease in intrusion attempts indicates a shift in attack tactics. The focus of cyber threats is shifting from technical intrusion attempts to exploiting the human factor (phishing, fraud) and using malware to steal credentials.

Investment scams using deepfakes of celebrities and "success stories" on fake portals dominate; malicious use of Google Ads and the impersonation of authoritative institutions is also widespread.

A public opinion survey conducted by CERT.LV[4] on cybersecurity awareness and habits in Latvian society reveals that more than half (66%) of the population has encountered fraudulent activities in the digital environment. The most common reasons for falling victim to fraud are acting in haste without proper evaluation (21%) and the perceived credibility of the fraudulent communication and its content (19%).

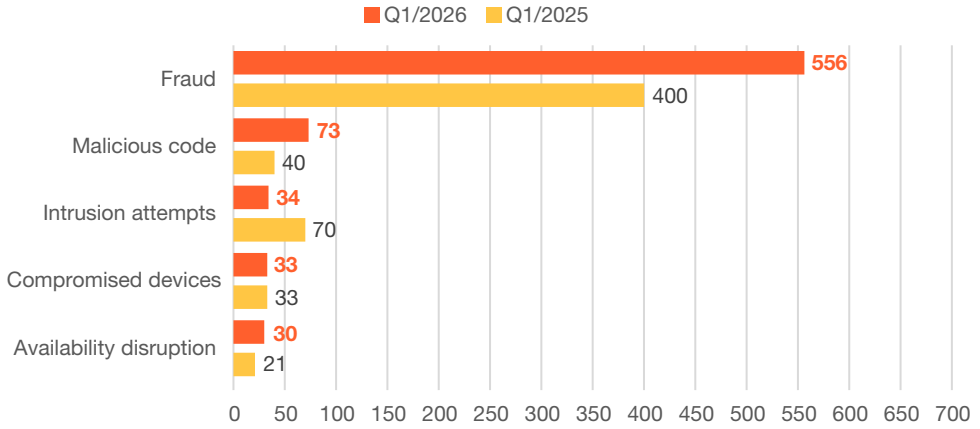

Figure 3. TOP 5 cyber incident types (number)

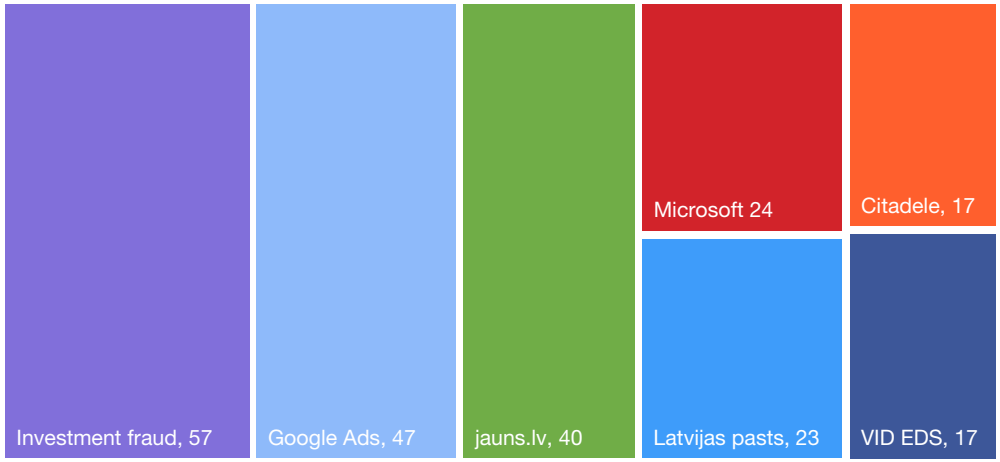

Figure 4. Most common fraud campaigns and themes (number)

4 The study was conducted at the end of 2025 in cooperation with the research company SIA "TNS LATVIA" (Kantar; now – Fifty5Blue).

CERT.LV invites everyone to use the platform kibertests.lv, designed for individuals and organisations to assess their basic cybersecurity knowledge and identify areas for improvement. At the same time, kibertests.lv can serve as a preparatory step before conducting phishing tests, providing organisations with an overview of their current situation and areas requiring improvement.

TOP 10 malware

The most widespread malware types in Q1 2026 indicate large-scale, automated, and persistent threats.

“Android.badbox2” continues to dominate the TOP 10 malware list, with its prevalence increasing by 58% compared to the previous quarter.

“Android.badbox2” is a mobile botnet variant capable of infecting devices, for example, by stealing credentials and enabling remote control. Its spread indicates significant and targeted activity on Android devices and points to mass infection campaigns using unofficial app installations or fake updates.

The main risks are the interception of access credentials, compromise of infected end devices, and their use in subsequent cyber-attacks. Organisations and individual users may not even be aware that their IP address is “participating” in botnet attacks.

The remaining top malware together account for a quantitatively smaller share; however, they demonstrate a diverse combination of attack vectors and increase compromise risks.

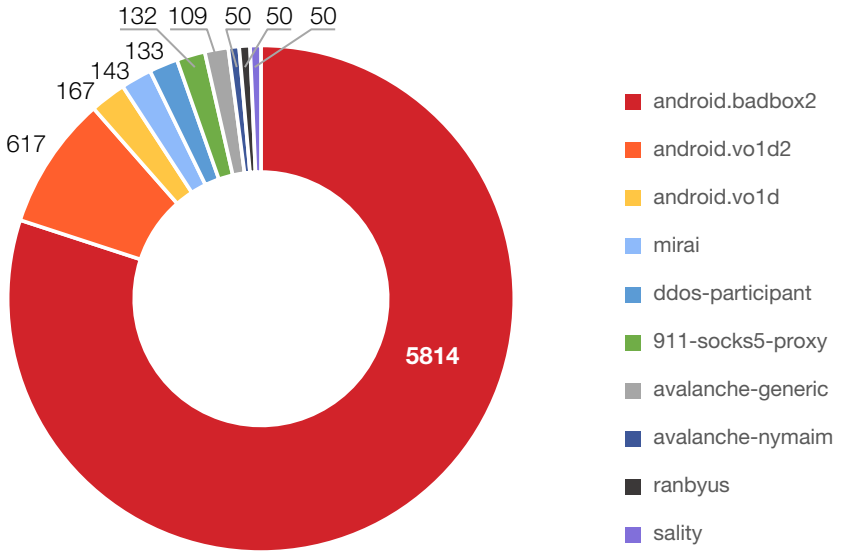

Figure 5. TOP 10 malware (number)

TOP 10 cyber-attack trends

- **Targeted phishing tailored to specific contexts is rapidly increasing**. Attacks occur when users search for specific services (e.g., VID EDS, e-health) in a browser. Phishing is becoming precisely aligned with user intent. Through the malicious use of Google Ads, users are redirected to fake websites.
- **Technological evolution and diversification of social engineering continue**, including fake CAPTCHA prompts that trick users into installing malware, fake software updates, and multi-channel attacks (email, phone, web) designed to manipulate users psychologically.

The most common types of malware

- **User data-stealing malware**
- **Botnets**
- **Remote control trojans for data extraction and infrastructure compromise**

“Infostealer” type data-stealing malware is used to extract access credentials from web browsers or unencrypted files. It is distributed as malicious browser extensions or executable files attached to phishing emails.

- **Malicious browser extensions that masquerade as legitimate tools** but actually perform harmful actions (collect passwords, session cookies, and other data).
- **Malware designed to extract user authentication data and compromise accounts**. Attack focus is shifting from infrastructure to end users. Information-stealing malware dominates – it extracts saved browser passwords and session access data. Several cases have been identified in Latvia, including situations where executable files were downloaded and run from the web. The number of phishing emails with malicious attachments has also increased. International sources indicate a significant increase in stolen credentials on illegal marketplaces in 2025, pointing to the active trading of such data.
- **Automation in attacks is increasing**. Phishing combined with malware and attacker-controlled command and control (*Command and Control / C2 servers*) enables attacks to be carried out quickly, cheaply, and at scale, making them harder to prevent.
- **A new automated mass fraud tactic using "silent call" techniques**. This is a technically simple but effective preparatory phase where "silent calls" are used to validate active phone numbers, marking a shift towards large-scale data collection.
- **Continuous "testing" of critical infrastructure**. Large-scale distributed denial-of-service attacks ("carpet bombing") have been observed, where attackers overload a wide range of targets simultaneously with high traffic volumes. This indicates a growing background level of automated threats. Periodic terabit-scale attacks have been observed targeting telecommunications infrastructure, demonstrating extremely large and powerful attack volumes.
- **The increase in ransomware poses a high risk to impact and business continuity**. Several cases have been recorded in Latvia, including the "HardBit" incident targeting a company's accounting server.
- **Business Email Compromise (BEC) with high financial impact**. One of the most effective financial attack methods (compromising executive email accounts, fake invoices/payment requests). Real cases with significant financial losses for companies have been recorded in Latvia.
- **Compromise of communication platforms**. Attacks are shifting towards secure communication platforms (e.g., account takeovers in Signal). Targets include officials representing Latvia internationally and journalists. This creates high risks of data leakage and potentially favourable conditions for espionage.

Attacker motivations

- **Financially motivated cyber-attackers:** main directions – ransomware, BEC, investment fraud, and data monetisation to generate profit or other benefits.
- **Politically motivated and state-sponsored attackers:** main directions – DDoS attacks against high-value targets; cyber-attacks against industrial control systems; attempts to compromise accounts of public international figures; intelligence gathering and access to sensitive information. Increased risk of information influence operations ahead of the 2026 parliamentary elections.
- **Opportunistic cyber-attackers:** focus on visible targets – government institutions, strategic organisations, public services. Use DDoS as a low-barrier impact tool. Activity is often not directly attributable, but target selection indicates strategic intent.

Regional threat context

- **Russia** remains the primary source of cyber threats. Russian hacktivist activity (often linked to and observed following public expressions of support for Ukraine in Latvia's media space) is expected to continue. The impact of these attacks is still assessed as low. The main risks are related to reputational damage to state institutions and influence on public opinion and the information space. Attacks may disrupt the operation and availability of targeted websites for the public.
- Activity of groups linked to **China** (PRC) with economic motivations (data acquisition, access to technologies); increasingly intensive attempts to spread within networks and access sensitive information.
- Occasional involvement of **Belarus**, mainly as part of Russia's "orchestrated" hybrid operations.
- There is a risk that **Iranian** hacktivist groups could become active in Latvia's information space if support for Israel is expressed. A similar pattern has already been observed with Russian hacktivist activity intensifying in response to Latvia's support for Ukraine.

Targeted sectors

Increasing risks related to threats to operational technologies (OT), which are used to monitor and control physical processes, equipment, and infrastructure essential for critical services such as **energy, water supply, and transport**.

Cyber-attackers can remotely access industrial control systems or other OT to influence service delivery if cybersecurity measures are insufficient.

Other targets include state and local government institutions, defence and political sectors, telecommunications, retail, and academia. Organisations with high public visibility and large customer bases are also at risk.

Impact on society, organisations, and the state

Three mutually reinforcing risks characterise the Latvian cyberspace.

- **Service availability disruptions**. Examples of key targets (LVRTC, "Tet", e-health) show that DDoS is not theoretical, but a daily operational risk. Periodic terabit-scale attacks are observed in Latvia, testing system limits and also serving as retaliation for Latvia's support for Ukraine.
- **Information-stealing malware and user account compromise**. Attack focus is shifting from infrastructure to end users. A case concerning a Microsoft tenant account compromise in a municipality demonstrates that such attacks can have a wide-reaching impact.
- **Supply chain and outsourcing risks**. Some organisations in Latvia still use strategically questionable solutions. For example, an incident where an accounting server used for a 1C warehouse system was compromised and infected with "HardBit" ransomware clearly showed that such choices are not only an IT issue but also a business and national security issue. The country of origin of 1C accounting software is Russia, and choosing such a product is considered a strategic mistake and potential threat.

Key conclusions and recommendations

Cybersecurity threats in Latvia remain high and are increasingly focused on user compromise rather than solely infrastructure vulnerabilities.

DDoS attacks have become an ongoing operational risk, testing organisational availability and resilience. It is necessary to strengthen business continuity plans and infrastructure resilience.

Phishing, information-stealing malware, fake software updates, and malicious browser extensions dominate, enabling attackers to bypass traditional protection mechanisms. The main risks are related to credential theft and unauthorised access, especially in organisations with weak user security controls. The human factor and social engineering have become the primary attack drivers.

To mitigate the impact, priority should be given to strengthening endpoint security, resource capacity, user training, and supply chain control, while improving response capabilities and operational continuity in line with regulatory requirements.

Recommendations for organisational ICT security

- **Regularly carry out a comprehensive inventory of devices and systems to obtain a complete overview of the infrastructure, in order to timely detect and mitigate risks caused by outdated or unprotected equipment.**
- **Avoid the unnecessary exposure of IT resources to the public internet, providing access through secure solutions only, using multi-factor authentication solutions (MFA) or encryption.**
- **Regularly follow software updates, promptly installing the latest available security patches for all systems.**
- **Implement centralised update management, ensuring continuous monitoring across all systems.**
- **Regularly perform vulnerability scanning to identify weaknesses and reduce risks from known vulnerabilities.**

3. CERT.LV services: protection and testing

3.1. DNS firewall

CERT.LV DNS firewall, using its maintained lists, in Q1 2026 **blocked access to malicious websites more than 2.5 million times** – this is:

- 139% more than in the previous quarter;
- 416% more than in the same period last year.

Possible reasons for the increase include seasonal and contextual factors, and the number of blocks is directly influenced by the number of active fraud campaigns.

CERT.LV proactively monitors and disrupts identified fraudulent campaigns. Public involvement is also important – users forward phishing emails, SMS messages, and malicious links to cert@cert.lv or report them via the phone on 23230444. Received reports are aggregated and verified, and malicious domain names are added to the DNS firewall to restrict access by Latvian internet users and reduce potential harm.

Major active defence episodes during the reporting period.

- Use of “Jauns.lv”, “DELFI”, and “LSM” branding in fraudulent cryptocurrency investment platform advertising campaigns;
- Use of “CSDD” and “SEB” branding in fake website campaigns.

The DNS firewall and its mobile application are available free of charge to all residents and organisations in Latvia. Additional information on installing the DNS firewall is available at dnsmuris.lv.

~280 K – Average number of blocked malicious websites per month
~30 min. – Average response time to identify malicious sites and add indicators to the blocking list
>84 K – DNS firewall mobile app downloads on Android and iOS devices (since 2024)
~5,6 M – Number of DNS requests in Q1 2026

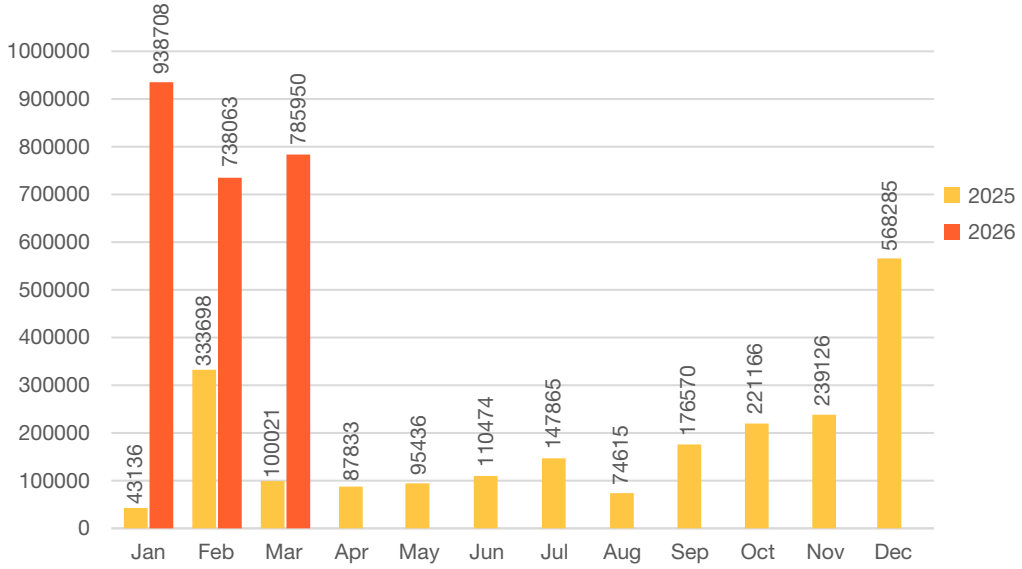

Figure 6. Malicious websites blocked by CERT.LV DNS firewall maintained lists (cert-shield, malware, phishing, high-risk*)

3.2. Threat early warning system (EWS)

The Cybersecurity Early Warning System (EWS) is a service provided by CERT.LV that analyses traffic anomalies and identifies signs of cyber-attacks in the service recipient’s infrastructure. CERT.LV continues to maintain and expand the EWS system.

The service includes:

- continuous analysis of data flow anomalies and detection of malware activity;

* This statistic does not include data from lists maintained by other competent national authorities for restricting illegal online content.

- sending alerts to service recipients about identified high-priority cyber threats;
- regular updates of CERT.LV cyber threat indicators;
- consulting and support for service recipients.

Detection and prevention of cyber threats and incidents

In Q1 2026, the number of alerts registered by EWS was approximately 872 million – this is:

- 9% more than in the previous quarter;
- approximately 2.52 times less than in the same period last year.

The decrease in volume is explained by the optimisation of the indicator set used.

The most relevant threats were related to network requests to domains associated with identified phishing campaigns, as well as malware prompting downloads of fake software updates. Network requests to identified malicious attacker-controlled command and control servers were also detected.

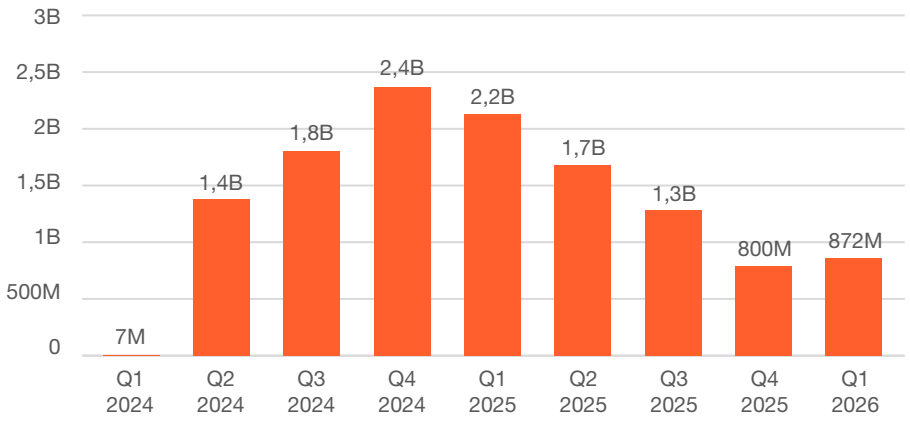

Figure 7. Number of EWS alerts by quarter (million – billion)

3.3. Security Operations Centre (SOC)

Implementation of the SOC service

CERT.LV continues to develop SOC services and attract new clients, expanding the client base in line with the NCL and strengthening effective protection and resilience against cyber threats.

The CERT.LV SOC service centrally collects security telemetry from client infrastructure and correlates events with the full set of threat indicators and knowledge available to CERT.LV to ensure the timely identification, alerting, and mitigation of cyber threats or incidents.

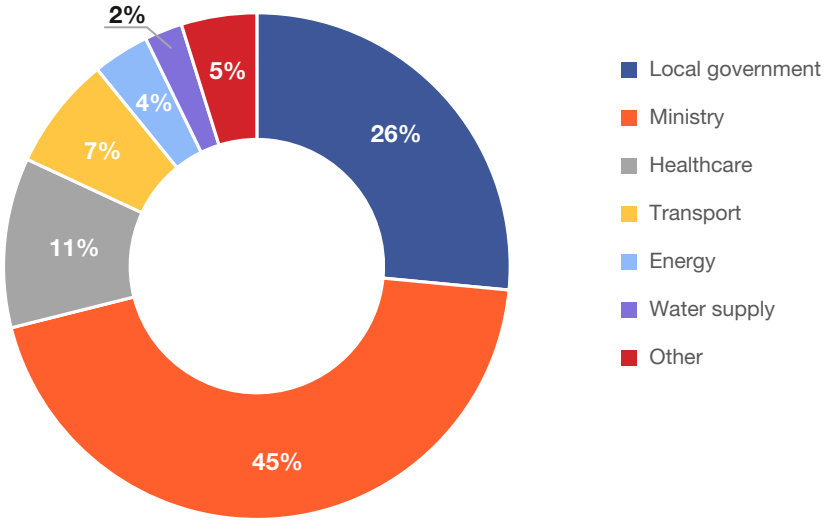

Figure 8. Distribution by sectors of institutions using CERT.LV SOC

As of the end of Q1 2026, CERT.LV SOC services are used by: **92 NCL entities** (increase of 37).

The growth in the number of SOC clients is also partly influenced by differences in statistical methodology – accounting is based on institutional registration numbers, meaning that subordinate institutions are counted separately if they have their own registration number and are registered as NCL entities.

Visibility has been achieved over 43,037 endpoints, including servers and workstations. During the reporting period, this represents a 3.6% increase, resulting in a higher number of security alerts.

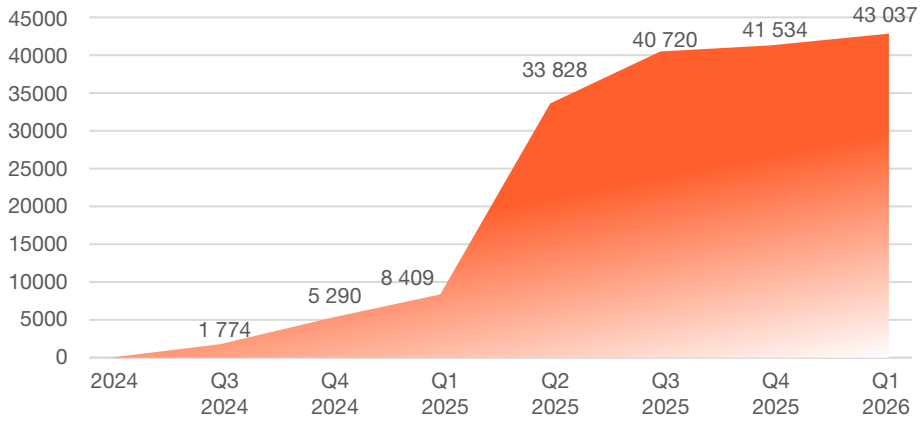

Figure 9. CERT.LV SOC visibility dynamics: number of endpoints

Detection and prevention of cyber threats and incidents

Indicators	Quantity	Change compared to Q4 2025
Total number of security alerts registered within the CERT.LV SOC service in Q1 2026:	**~24 million**	**+4%**
Low level of alert	**~6 million**	**-11%**
Medium level of alert	**~18 million**	**+8%**
High level of alert	**~11 thousand**	**-86%**
Critical level of alert	**~16 thousand**	**-70%**
Manually created cases	**586**	**+13%**
False positive cases	**571**	**+12%**
Number of cyber incidents	**15**	**+88%**

During the reporting period, **approximately 24 million security alerts were registered**, representing a **4% increase** compared to Q4 2025. The increase is mainly explained by improved visibility in the infrastructure of new clients.

Most alerts were of medium severity (~74% of the total), and their number increased by 8% compared to Q4 2025. Low-level alerts (~25% of the total), mainly related to system noise and false positives, decreased by 11%.

Overall, an improvement in alert processing quality is observed, reducing the proportion of insignificant events.

The absolute number of high and critical alerts (~27 thousand) decreased almost fivefold compared to Q4 2025 (~133 thousand).

High and critical alerts indicate potentially dangerous attacks and require careful evaluation, with particular attention paid to critical-level alerts.

The decrease in alerts is influenced by the effectiveness of implemented security measures in client environments, as well as the improved identification of false positives. The reduced alert volume enables the earlier identification of real risks and supports the systematic strengthening of cybersecurity resilience.

Cases created within the SOC service and recorded cyber incidents

Within the CERT.LV SOC service in Q1 2026:

586 (+66) – Manually created cases

571 (+59) – False positive cases

15 (+7) – Recorded incidents across 13 different institutions

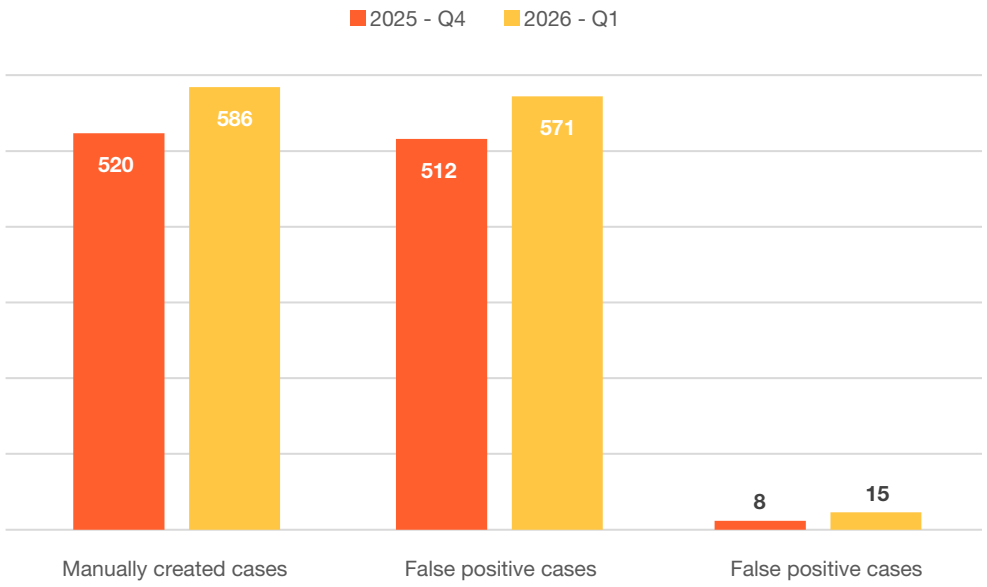

Figure 10. Structure and comparison of security events

Overview of cyber incidents recorded during the reporting period

The most extensive incident was detected simultaneously in four institutions, where suspicious activity indicated possible malware infection via phishing. In total, 6 devices were affected, all of which were within SOC monitoring visibility.

Antivirus software was used in all affected environments, but in this particular case, it was unable to prevent the malware from executing. The incident was escalated for further investigation and impact assessment.

During the investigation, an additional infected device was identified in another institution where SOC telemetry data was not available. Considering the scale and potential impact, alerts were sent to clients, and an informational notice was published on social media.

Other identified incidents were mainly related to downloading and executing unwanted or uncontrolled software, information-stealing malware, brute-force attacks, and the unintentional exposure of unsecured endpoints to the internet, potentially placing them at risk.

Recorded incidents were mainly related to user actions and weak security practices, with the most significant risks being the human factor and insufficient access control. This indicates the need to prioritise user training, access control, and endpoint security as key protection areas.

The CERT.LV SOC service supports timely threat detection and response, improving organisations' ability to ensure continuous, effective protection and resilience against cyber threats in 24/7 mode.

Dominant initial access vectors:

- **phishing and malicious email attachments;**
- **browser plugins;**
- **fake "CAPTCHA";**
- **executable files downloaded and run from the web;**
- **removable media (USB), executed files.**

3.4. Cybersecurity threat hunting operations

Since 2022, when threat hunting operations began, by the end of Q1 2026, a total of **164 000 endpoint devices** across more than 42 NCL entities (including critical ICT infrastructure organisations) have been analysed.

The data shows that APT presence was identified in approximately 20% of the organisations analysed during threat hunting operations.

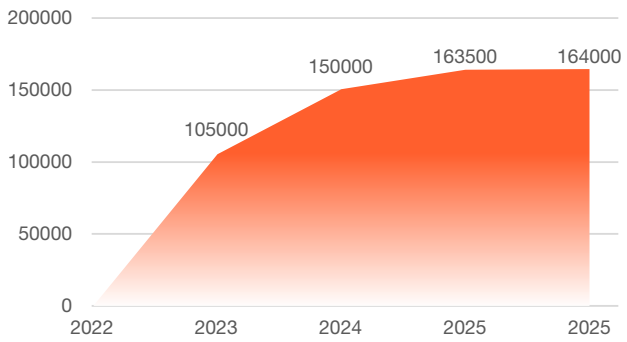

Figure 11. Dynamics of the volume of devices analysed during threat hunting operations

Bilateral strategic cooperation

Latvia – Canada

CERT.LV continues its strategic partnership with the Canadian Armed Forces Cyber Command in organising threat hunting operations.

From 24–27 March in Riga, CERT.LV and the Canadian Armed Forces Cyber Command organised the fourth **Threat Hunting training course**, led by cybersecurity specialists from Canada and Latvia. The event brought together 37 participants from 14 countries to strengthen their ability to act proactively and identify cyber threats before they materialise. The training course was implemented with financial support from the European Union (EU) under the CERT.LV-SOC-LV project.

Photo: Amy Langlois

Latvia – Ukraine

Strategic cooperation with Ukrainian cybersecurity institutions continues, jointly developing cyber defence capabilities, ensuring ICT infrastructure protection, and integrating Ukraine's experience gained in the war against Russia. More: **Latvia and Ukraine sign a letter of intent on cooperation in establishing a regional cybersecurity centre in Ukraine**.

Photo: Ministry of Defence

On 19 February in Kyiv, Ukraine, at the Kyiv International Cyber Resilience Forum 2026, CERT.LV expert Mārtiņš Savickis led a one-day threat hunting workshop and delivered a presentation "Threat Hunting in Latvia: Proactive Defense of Critical Infrastructure" on threat hunting and its results in Latvia. The forum was

3.5. IT system security tests and phishing attack simulation campaigns

IT system security tests

In Q1 2026, CERT.LV conducted **10** IT system security tests, identifying a total of **22** vulnerabilities, including **7** critical ones, which have already been mitigated thanks to the security tests.

CERT.LV provides:

- network security analysis;
- software vulnerability assessment;
- web application security assessment;
- IT infrastructure vulnerability assessment;
- consultations and recommendations for improving security.

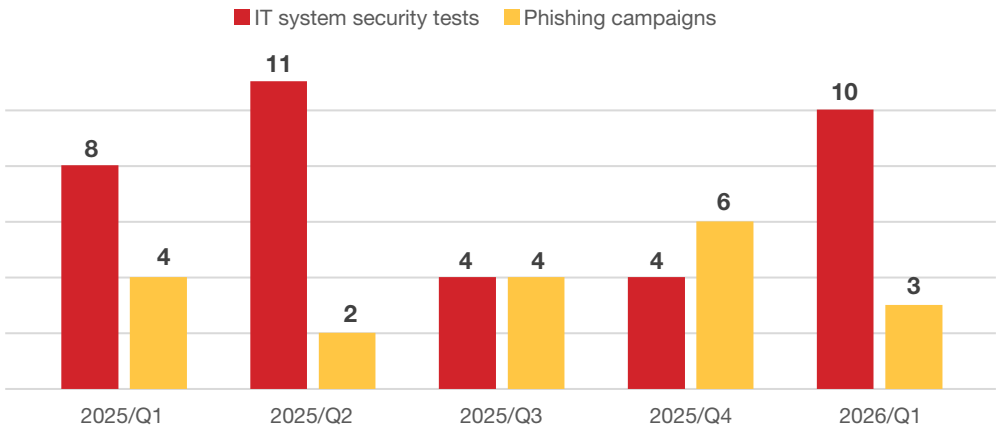

Figure 12. IT system tests and phishing attack simulations

Phishing attack simulation campaigns

During the reporting period, **3 phishing simulation campaigns** were conducted to train employees and improve their ability to recognise risky behaviour, identify cyber threats, and prevent data leakage. A total of **912 emails** were sent as part of these campaigns.

Phishing simulations significantly strengthen organisational resilience against social engineering attacks and reduce human-related risks.

3.6. Vulnerability Reporting Platform (CVD)

The CVD platform is intended to facilitate cooperation between state and local government institutions and cybersecurity researchers and to improve the security of ICT resources. Using the CVD platform, an institution can register information on all ICT resources it uses for which it wishes to receive reports on identified vulnerabilities. The platform provides a transparent and user-friendly interface where all received reports can be viewed, and communication with researchers and other involved parties can be maintained.

By the end of Q1 2026, the CVD platform had registered:

- **166 security researchers** (increase of 18);
- **14 active institutional programmes** (new participant – State Revenue Service);
- **541 vulnerability reports** (increase of 107), including:
  - ✓ **355** vulnerabilities in CERT.LV client systems (increase of 93);
  - ✓ **186** vulnerabilities reported within specific institutional programmes (increase of 14).

See the active institutional programmes at: cvd.cert.lv.

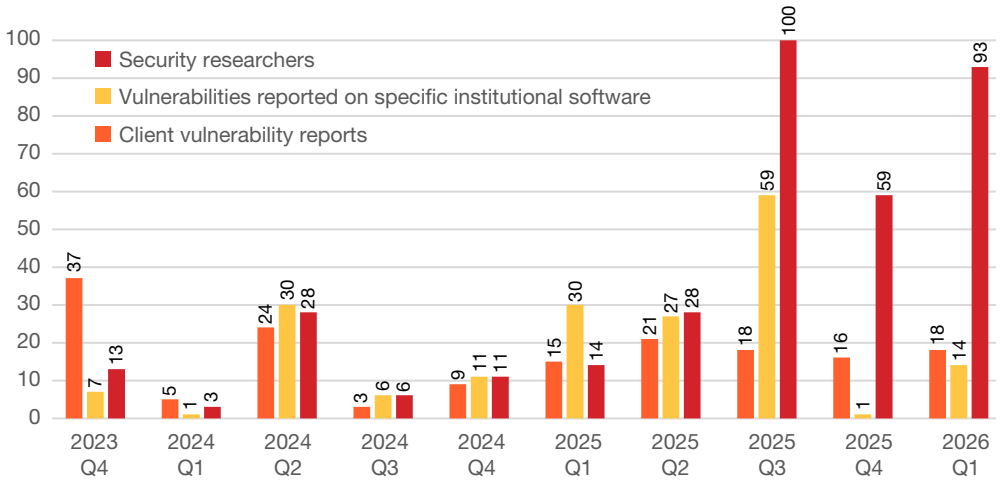

Figure 13. CVD: Trends in the growth of security researchers and vulnerability reports

3.7. Operational Technology (OT) Security

Activities

CERT.LV has established cooperation with operators in Latvia's energy, water supply, heat supply, and transport sectors, and has concluded operational technology (hereinafter – OT) security service agreements.

The promotion of OT system security takes place in three main directions: **system monitoring and anomaly identification, security testing, and incident response**.

- Within system monitoring, CERT.LV has installed five OT network data flow monitoring sensors, and active preparations are underway to expand them. In parallel with monitoring internal OT network communications, activities are carried out for the continuous monitoring of Latvian IP address networks with the aim of identifying publicly exposed systems, assessing their potential vulnerabilities, and performing the coordinated restriction of access and remediation of deficiencies.
- Within OT system component security testing, activities are carried out to test the security of various smart and industrial control devices in order to identify potential vulnerabilities or supply chain weaknesses that could allow the unauthorised control of these devices and overall systems by manufacturers or external attackers. Initial checks are carried out on equipment originating from China. Over the past year, such equipment has included remotely controllable smart devices (e.g., smart meters and mobile communication modems) and electric vehicle charging stations.
- Broader cooperation has been established with cybersecurity authorities of the Nordic and Baltic countries (NB8).

Threats, incidents, impact

Early identification of potential risks and vulnerabilities, proactive action, and the mitigation of their impact are carried out.

The overall situation of resilience of Latvia's operational systems against cyber-attacks is assessed as adequate, with a steady trend of improvement. As a result of regular activities, private or small-scale OT systems accessible from the internet are identified, and operators are informed and engaged in cooperation to reduce or eliminate the potential impact.

A continuous threat from states unfriendly to Latvia is expected, aiming to gain control and carry out destructive actions in critical infrastructure operator systems. To mitigate such risks and make Latvia a more difficult target, CERT.LV will continue work on OT activity areas, ensuring broader visibility and threat identification, the execution of security tests, and coordinated incident response.

4. Strengthening cybersecurity through society-wide measures

By promoting awareness and strengthening users' knowledge and skills in cybersecurity, including those of organisational employees, CERT.LV experts educated a total of **13 309** participants across **65** events and activities in Q1 2026. This represents an increase of 32 events and 3 104 participants compared to the same period last year.

CERT.LV in Q1 2026:

- organised a webinar for IT specialists **"Effective Windows Firewall Management"**, during which CERT.LV experts explained how to properly configure the Windows firewall in a corporate environment using Group Policy (GPO) to effectively protect endpoints, even outside the organisational network, and reduce cybersecurity risks. Slides from the webinar are available on the website **cert.lv**;
- organised the IT security seminar **"Esi drošs! (Be Safe!)"**, bringing together more than 500 participants, both in person and online. The seminar took place within "Digital Week Latvia 2026" and covered practical and current issues related to the registration of NCL entities, actions in the event of a cybersecurity incident, as well as provided insight into threat hunting processes, employee phishing tests, the most common "cyber weather" observed in 2025, and vulnerability disclosure processes. The recording and slides from the seminar are available on the website **cert.lv**;
- organised a continuing education seminar for teachers, held in cooperation with LIKTA within "Digital Week Latvia 2026". The aim of the event was to discuss current cybersecurity topics and to rehearse and prepare participants to run the cyber investigation game "Find the hacker at Livonia Secondary School" for upper primary and secondary school students.

More detailed information about CERT.LV lectures, training games and educational activities is available in the "Services" section of the CERT.LV website.

5. Overview of the activities of the LIA Safer Internet Centre Report Line

The Latvian Internet Association Safer Internet Centre Report Line (RL) has received and evaluated **340** reports between 01.01.2026 and 31.03.2026. Of these, **101** reports contained child sexual abuse material, **14** reports contained pornography without an age restriction warning, **19** reports contained defamation and slander, **4** reports contained hate speech, and **5** reports contained violent material. There were **48** reports of attempted financial fraud on the internet, **117** of which were not illegal in content, and **32** of which resulted in recommendations to whistleblowers to resolve the problem.

22 reports of hate speech and child sexual abuse material hosted on servers in Latvia were sent to the National Police. **62** reports of child sexual abuse material originating outside Latvia have been entered into the INHOPE Association's database and submitted to the relevant INHOPE country reporting line for follow-up action to remove illegal content from the public domain.

During the reporting period, out of **22** reports of child sexual abuse material hosted in Latvia, content in **20** cases has been removed from public access, while **2** cases remain in the removal process.

Overview of reports received from 01.01.2026 to 31.03.2026

Reports	Jan-26	Feb-26	Mar-26	Q1
Erotic / pornographic content without age restriction warnings	6	3	5	14
Child sexual abuse / child prostitution / child sexual exploitation material	40	27	34	101
Violent content	1	3	1	5
Defamation / insult	7	10	2	19
Hate speech / racism	0	1	3	4
Financial fraud	20	9	19	48
Consultations / advice	10	11	11	32
Other	38	49	30	117
TOTAL:	122	113	105	340

Reports sent to the State Police	9	3	10	22
Reports sent to the INHOPE association	22	21	22	65
TOTAL SENT FOR REVIEW:	31	24	32	87

CERT.LV's mission is to promote cybersecurity in Latvia.

The main tasks of CERT.LV are to maintain and update information on cybersecurity threats, provide support to state institutions in the field of cybersecurity, assist in resolving cybersecurity incidents for any natural or legal person if the incident involves a Latvian IP address or a .LV domain, as well as to organise informational and educational events for government employees, IT security professionals, and other interested parties.

The report includes publicly available information and does not contain any restricted information. This report is for information only.

Contact CERT.LV:

Phone: +371 67085888

E-mail: cert@cert.lv

Website: www.cert.lv

Follow CERT.LV news on:

@cert.lv